Association for Information Systems
AIS Electronic Library (AISeL)

CONF-IRM 2016 Proceedings

International Conference on Information Resources Management (CONF-IRM)

2016

Adoption of Big Data Solutions: A study on its security determinants using Sec-TOE Framework

Khairulliza Ahmad Salleh
The University of Auckland, k.salleh@auckland.ac.nz

Lech Janczewski
The University of Auckland, lech@auckland.ac.nz

11. Adoption of Big Data Solutions: A study on its security determinants using Sec-TOE Framework

Khairulliza Ahmad Salleh
The University of Auckland
k.salleh@auckland.ac.nz

Lech Janczewski
The University of Auckland
lech@auckland.ac.nz

Abstract

Big Data Solutions (BDS) refers to innovative solutions designed to perform searching, mining and analysis of high volume of data. While BDS is being actively adopted by pioneering and leading organizations due to its prospective benefits, many organizations are still divided on the need to adopt it. Security issues related to big data's characteristics are among the hindering factors cited by non-adopters. Thus, it creates opportunities to study on the security related issues pertinent to BDS adoption. In this preliminary study, Technology-Organizational-Environmental (TOE) framework was adopted and adapted to fit the security factors being studied. Data were collected from 25 respondents through an anonymous online questionnaire and descriptive analysis was performed. The results reveal that an organization's intention to adopt BDS can be positively influenced by perceived compatibility, top management support, information security culture and organizational learning culture. Whilst, the non-adopters are negatively influenced by perceived complexity and risks in outsourcing. One factor was found to have inconclusive outcome to both adopters and non-adopters (security and privacy regulatory concern), suggesting that it may not have any significant effects in organizational intention to adopt BDS.

Keywords

Security and Privacy, Big Data Adoption, Big Data Solutions, TOE Framework, Quantitative Method

1. Introduction and research question

Big data is a term that emerged in the last few years and its associated technologies are now relevant across industries and economic sectors. This phenomenon is in part due to the proliferation of digital data; in addition to the vast amount of data being produced by data-intensive organizations. While the technologies that supported big data has been one of the most talked about technology trends in recent years, there is still no concrete definition to the term big data itself. Hence, the term is normally described by practitioners and researchers according to its traits. The common associated traits are: "volume –large amount of data", "variety – different types of data collected", and "velocity – speed of data transfer and creation" (Bansal, Kaur, & Aggarwal, 2014) . However, one common view can be derived; big data consist of huge data sets, with various data types and sources produced and transferred at great speed. These characteristics create a difficulty in managing and processing data using traditional data

processing techniques or saving it in any traditional structured relational database management systems.

To fully harness the potential of big data, organizations are starting to seek for technologies and solutions that have the ability to process and analyse these various sources of data and data types (Davenport & Dyche, 2013). Technologies and solutions for big data such as Hadoop systems are now available for selection and deployment by organizations. Looking at the benefits of deploying big data solutions (BDS) specifically in terms of its ability to store, accumulate and combine large datasets, organizations are now well aware of how big data will enable rigorous data processing, thus making deep analyses of data more accessible (Wielki, 2015). Pioneering business and organizations have started to exploit the benefits of big data in creating value for their operation in order to remain competitive. These early adopters of BDS are aware of its potential to open up new business opportunities and provide better understanding of their business setting.

Even though some organizations are already on the "forefront of big data analytics and thus are highly bullish" about its benefits and prospects, there are still a large segment of industries that have separate view over big data's purported values (Kwon, Lee, & Shin, 2014). A recent Enterprise Big Data survey conducted by IDG Enterprise shows several issues cited by the respondents as the factors that inhibit the adoption of BDS. Among others, security and privacy issues were found as one of the hindering factors (IDG Enterprise, 2014). In other surveys conducted by market research companies and technology providers, security and privacy issues have also consistently been named as one of the top hurdles or challenges in organizations' big data efforts (Gartner Inc, 2014; Sans Institute, 2015). This finding demonstrates that business and IT executives believe BDS may posed new security threats and challenges, as commonly encountered during new technology adoption in organizations (Kshetri, 2014). Accordingly, having BDS installed does not only require effective management of storage and retrieval of data, as it also encompass the need to address the various privacy issues and security-related threats. The threats unique to BDS may be contributed by the characteristics of big data itself; the variety, velocity and volume of data. These unique characteristics magnifies the challenges for managing big data security as opposed to managing traditional data environment (Nasser & Tariq, 2015). Else, the security features of BDS such as the open-source Hadoop is also lacking in its initial design. It was evidently not designed with security features in mind, as it was solely intended to handle large data storage and fast processing. Regardless of Hadoop's security weaknesses, it is presently receiving wide integration with organizations' existing IT infrastructure and consequently introduces security vulnerabilities (MIT Technology Review, 2015).

While there is a growing number of publications that report on privacy and security issues in relation to big data, the number of empirical findings on its adoption by organizations and its associated security factors that may influence the intention to adopt is still scarce (Ahmad Salleh, Janczewski, & Beltran, 2015; Kshetri, 2014). Although it is safe to conclude that Big Data solutions are gaining momentum in its acceptance and importance across industries, there are still security issues and challenges in relation to big data, which dampens the adoption by certain businesses and organizations. Can the deterring factors be attributed to diverse perception on the complexity of securing big data environment, a lack of top management support in acknowledging the importance of information security for new adopted technology, or the need to comply with security and privacy related regulations? These issues create research

opportunities to comprehend the security related factors pertinent to big data adoption in organizations. It is therefore the aim of this study to look into adoption factors, specifically from security aspects that may encourage or discourage the adoption of BDS. Theoretically, this study applies the TOE framework (Technology-Organization- Environment) by Tornatzky and Fleischer (1990) to answer the following research question: *How do technology factors in security, organizational security view and security-related environmental factors encourage/discourage organizations' big data solution adoption?* This paper presents the preliminary descriptive findings of the study. The remainder of this paper is organized as follows: section 2 describes the conceptual research framework, followed by the research methodology in section 3. Section 4 presents the results from descriptive analysis and discussion. This paper ends with a section that concludes the findings, limitations of this study and details of planned future works.

2. Conceptual Research Framework

For the purpose of this study, an organizational level technology adoption framework – the TOE framework (Tornatzky & Fleischer, 1990), is adapted to align with the security factors that we believe influences BDS adoption in organizations (Sec-TOE framework). Figure 1 illustrates the conceptual framework for this study.

2.1 Sec-TOE Framework

The TOE framework is a general framework in innovation studies that describes three contexts that may influence the process of technological innovation adoption and implementation at organizational level. The three contexts are: technological, organizational and environmental (Tornatzky & Fleischer, 1990). To address the research question of this study, the TOE framework is adopted and the constructs under each of the three contexts are adapted to align with security related factors, hence the name Sec-TOE (Ahmad Salleh et al., 2015). The technological context refers to internal and external technologies relevant to an organization. As asserted by Tornatzky and Fleischer (1990), the fit between the existing technology setting in an organization and the intended technology innovation will be the determinant in the decision to adopt technology innovation. Thus, the main emphasis is on how the adoption process can be influenced by technology characteristics themselves (Chau & Tam, 1997). Two technological constructs were used in this study; *perceived complexity*, and *perceived compatibility.*

The TOE framework's second context is organizational. This context comprises of multiple characteristics that represent an organization in general. The characteristics may include organizational strategies, culture, structure as well as policies (Teo, Ranganathan, & Dhaliwal, 2006). These characteristics may either be a constrain or facilitating factor in the adoption of new technology by organizations (Oliveira & Martins, 2011). Organizational context for this study comprises of three constructs; *top management support*, *information security culture,* and *organizational learning culture*. The third context – environmental, refers to the domain "in which a firm conducts its business – its industry, competitors, access to resources supplied by others, and dealing with the government" (Tornatzky & Fleischer, 1990). Primarily, this context implies that there will be influences from the environment in which an organization operates when dealing with technology adoption. For this context, the constructs used were *security/privacy regulatory concerns* and *risks in outsourcing.*

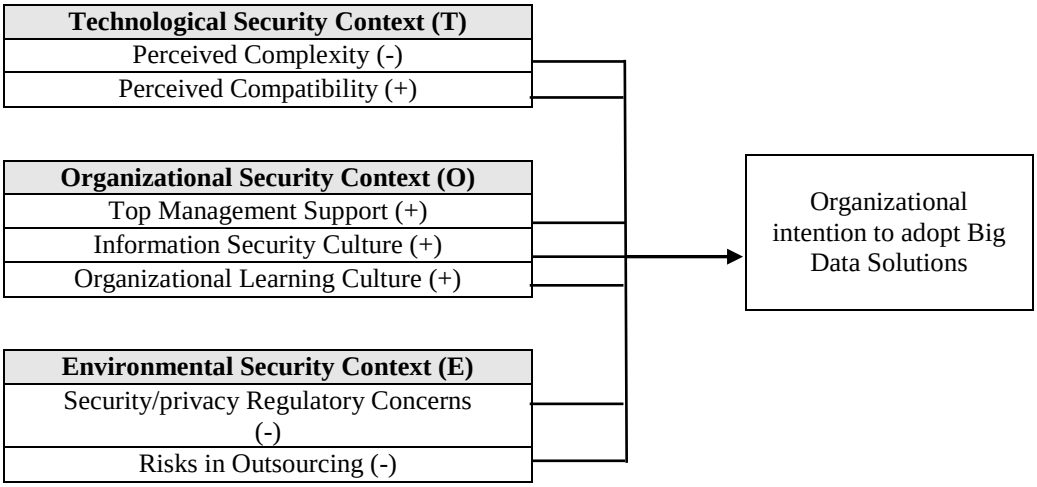

Figure 1: Sec-TOE Framework – Security determinants in BDS adoption

2.1.1 Organizational Intention to Adopt BDS

The dependent variable for this study is organizational intention to adopt BDS. In this context, BDS refers to a collection of technologies and framework that provides a "platform to integrate, manage, and apply sophisticated computational processing to big data" (Davenport, 2014, p. 120). BDS adoption signifies organizational intention and decision to select, install and implement BDS.

2.1.2 Perceived Complexity

Perceived complexity in the context of this study is defined as the perceived degree of difficulty and understanding in providing security mechanisms for BDS. Higher (perceived) complexity is normally associated with higher level of uncertainty in relation to successful adoption of new technology (Grover, 1993). In a big data environment, the need for security technologies and controls that is flexible enough to effectively address changing requirements may affect the perceived complexity as viewed by organizations. Thus, we postulate that a higher perceived complexity in ensuring the security of BDS will negatively affects organization's intention to adopt BDS.

2.1.3 Perceived Compatibility

The term 'compatibility' refers to "the degree to which an innovation is perceived as being consistent with the existing value, past experiences, and needs of receivers" (Rogers, 2003). In this study, perceived compatibility reflects the degree to which an organization's current security technology and control mechanisms are perceived as fit with the security requirements of BDS. As compatibility factor has consistently been found to exert influence in new technology adoption (Borgman, Bahli, Heier, & Schewski, 2013), this study posits that perceived compatibility of organization's present security technology and mechanisms with security requirements of BDS positively affects organization's intention to adopt BDS.

2.1.4 Top Management Support

This study defines top management support as the level of support and commitment given by organizations' top management towards IS security requirement and mechanisms involved in BDS adoption. With the support of top management, financial and technical resources are highly likely to be made available specifically for IS security. Additionally, organizational security awareness and policy enforcement will also be more effective (Hu, Dinev, Hart, & Cooke, 2012), thus creating a stable environment for new technology adoption such as BDS. Thus, it is expected that top management support for IS security will positively affects organization's intention to adopt BDS.

2.1.5 Information Security Culture

Information security culture denotes "the totality of patterns of behaviour in an organization that contribute to the protection of information of all kinds" (Dhillon, 1997). Within any big data environment, the handling of huge amount of data that comes from different sources and at a great speed will intensify organizational risks in being a victim of information security abuse. Human behaviour has consistently been cited as one the risks to information security abuse within organizations (Pahnila et al., 2007). Embedded information security culture may exert influence on employees to diminish human behaviour risks to information assets by protecting organizational information (Van Niekerk & Von Solms, 2010). For this reason, this study hypothesizes that embedded information security culture within organizations positively affects organization's intention to adopt of BDS.

2.1.6 Organizational Learning Culture

Learning characteristics and orientation of an organization is important during complex technology adoption process. By having a strong learning characteristics, an organization will have the ability to adeptly learn new technologies, scan for risks, identify opportunities and provide solutions (Nambisan & Wang, 1999). BDS for example, may require security personnel to identify new risks associated to it, and learn on new mechanisms for its protection. Considering this, organizations that exhibit a positive learning culture will decrease knowledge barriers that may deter BDS adoption. Hence, a positive organizational learning culture is anticipated to positively affect organization's intention to adopt BDS.

2.1.7 Security and Privacy Regulatory Concerns

Security and privacy regulatory concerns in this study refers to the degree of concern in ensuring compliance to security and data privacy regulations in relation to BDS adoption. Traditionally, data protection regulations is simpler to manage and adhere to since it were mostly created based on the foundation of structured data (Cumbley & Church, 2013). Big data otherwise, consist of mostly unstructured data, thus ensuring compliance to privacy regulations is far more complicated. This is turn, may result in significant reduction of interest in big data exploitation by organizations. For this, it is hypothesized that security and privacy regulatory concern negatively affects organization's intention to adopt BDS.

2.1.8 Risks in Outsourcing

This study defines risks in outsourcing as perceived degree of security and privacy risks associated to outsourcing (outsource BDS or the use of third-party tools). Organizations interested in embarking on big data initiatives may have to start with outsourcing the whole big

data environment or part of it. As BDS is relatively new, most organizations are still without the capability to build and maintain an in-house big data environment (Wood, 2013). The need to outsource may introduce security and privacy associated risks, a dependency towards vendors and organizations will need to relinquish some control of their information assets over to vendors. Thus, this study posits that risks in outsourcing negatively affect organization's intention to adopt BDS.

3. Methodology

Data for this study were collected using an anonymous online questionnaire survey administered in New Zealand. The questionnaire comprises of three sections. The first section consists of items relating to respondents' organizational background which includes a question on the level of BDS adoption in respondents' organization. The second section assesses organization's perception on technological, organizational and environmental security factors using a five-point Likert scale ranging from "Strongly Disagree (1)" to "Strongly Agree (5)". The questionnaire ends with one question that asks the respondents to rate their level of concern on BDS security from a scale of 1 to 10 (1=Low, 10=High) and an open-ended question on organization's main security and privacy concern on BDS based on any principles of the CIA triad. Survey items for each constructs were mainly identified from prior studies and adapted to the context of the study. The survey items were then reviewed by 2 academics in information systems field, 1 practicing information security professional and 1 doctoral student to ensure content clarity of the overall questionnaire. The survey was administered to New Zealand Information Security Forum (NZISF), a special interest group which members have a common interest in information security. Purposive sampling was used and deemed suitable for this preliminary study as it was intended to test the instrument and derive an estimation of results before the actual survey is administered. In total, 25 responses from 70 selected members were recorded, yielding a response rate of 35.7 percent. Given the small sample size, it does not allow for a robust parametric/inferential statistical analysis. Thus, this study primarily looked at descriptive analysis to explore the collected data.

4. Results and Discussion

Descriptive statistics of the respondents and their organizations are presented in Table 1. Most of the respondents were from organizations that have more than 2000 employees and are handling 1 to 100 terabytes of data per month. Out of the 25 valid responses, 15 (60%) are classified as adopters and 10 (40%) non-adopters.

Category	Frequency	Percentage (%)
Job Position		
• Chief Information Officer (CIO) / IT Director	1	4%
• IS/IT Management/Staff	13	52%
• Info. Security Management/Staff	8	32%
• Others	3	12%
Industry		
• Consumer Goods	3	12%
• Education	3	12%
• Energy and Natural Resources	1	4%
• Financial Services	2	8%
• Government/Public Sector	1	4%
• Healthcare/Pharmaceuticals	1	4%
• IT and Technology	9	36%

• Telecommunications	2	8%
• Others	3	12%
Number of Employees		
• Less than 50	1	4%
• 51-100	2	8%
• 101-500	2	8%
• 501-1000	6	24%
• 1001-2000	4	8%
• More than 2000	10	40%
Amount of Data Handled Per Month		
• Above 100 TB	2	8%
• 1 to 100 TB	7	28%
• 500 GB to 1 TB	4	16%
• 100 GB to 500 GB	2	8%
• Below 100 GB	2	8%
• Not aware of the amount	8	32%
BDS Adoption Level		
• Adopted	15	60%
• Do not adopt	10	40%

Table 1: Descriptive Statistics of Respondents and Their Organizations (N=25)

The results also reveal that adopters were mostly medium to large sized organizations and are managing 500GB to above 1TB of data per month. This finding shows that adopter organizations fulfilled the initial requirement of BDS implementation: having the *volume* of data to work with. Descriptive statistics and internal consistencies for the two constructs under *Technology* context are presented in Table 2. This study posits that a higher perceived complexity in ensuring security of BDS negatively affect the intention to adopt BDS. Findings show that perceived complexity is indeed higher for organizations classified as non-adopters (3.80) than the mean for adopters (3.22). The highest level of agreement for the non-respondents went to the item that states integrating security requirements of BDS in their current work practices will be very difficult (4.10). One measurement item – CX2, has high standard deviations for both adopters and non-adopters (>=1). This may imply high variance of perception on the complexity of skills required to secure BDS. Although the adopters' mean score (3.00) indicate uncertainty on the complexity of skills required, the high standard deviation shows that some respondents agreed on the skills complexity and some who did not. Different level of knowledge, experience and skills of the respondents in information security and complex technology in general, may be the factors that lead to this varied perception.

As for *perceived compatibility*, the assumption is that a perceived compatibility of an organization's present security practices and mechanisms with the security requirements of BDS will positively affect the intention to adopt it. Looking at the mean score for both adopters (3.42) and non-adopters (2.90), this assumption seems valid. Whilst the mean score is indeed higher for the adopters, a score of 3.42 is closer to 3.0 (uncertain scale), demonstrating that some adopters tended to be uncertain of the compatibility of their organization's present security practices and mechanisms with those of BDS requirement. Being a relatively new technology, potential security compatibility issues introduced by BDS might not be fully encountered and understood

by adopters. Else, compatibility issues might not be considered as significantly different from the adopters' normal operating challenges (Borgman et al., 2013).

Measurement Items (Perceived Complexity)		Adopters (N=15)		Non- Adopters (N=10)	
		Mean	Std. Dev.	Mean	Std. Dev.
CX1	Establishing information security mechanisms for BDS is difficult and complex	3.40	.910	3.70	.675
CX2	The skills required to secure BDS are too complex for our employees	3.00	1.0	3.60	1.075
CX3	Integrating security requirements of BDS in our current work practices will be very difficult	3.27	.704	4.10	.568
	Cronbach's Alpha = 0.812 **Total**	3.22	.452	3.80	.447
(Perceived Compatibility)					
CP1	The changes introduced by BDS is compatible with the organization's existing information security practices	3.40	.828	3.00	.444
CP2	Security requirements of BDS is compatible with the organization's existing information security infrastructure	3.40	.828	2.80	.844
CP3	Development of info security mechanisms for BDS is compatible with the organization's existing experiences with similar systems.	3.47	.743	2.90	.989
	Cronbach's Alpha = 0.864 **Total**	3.42	.375	2.90	.390

Table 2: Descriptive Statistics for Perceived Complexity and Perceived Compatibility

Table 3 presents the means, standard deviations and internal consistencies of all three constructs under *Organizational* context. From the table, it can be seen that the means of *top management support* for non-adopters clearly falls behind the means of the adopters (2.88 vs 3.84). The findings seem to show an agreement towards the assumption that top management support for IS security will positively affect the intention to adopt BDS. This suggests that commitment and support from the top management will indeed create a conducive environment for adoption of new technology innovation (Borgman et al., 2013). Support given by top management through effective communication and tolerance towards newly introduced risks will help in providing the necessary security mechanisms required by less mature technology such as BDS.

The mean scores for all items measuring *information security culture* were relatively high for adopters. These high averages suggest the existence of information security culture in adopters' organizations. As can be seen in the table, there's a difference in the total means for adopters (4.01) and non-adopters (3.53). With this, support is given to this study's initial proposition that embedded information security culture within organization will have a positive effect towards intention to adopt BDS. Embedded information security culture as part of organizational traits will help to instill security awareness among employees and thus helping the organization to avoid security risks associated to human behavior (Lim, Ahmad, & Maynard, 2010). Consequently, this culture will lead to an improved security level for the whole organization, making it more secure to host data intensive technologies such as the BDS.

Similar results were shown for *organizational learning culture*. Comparing the means for adopters and non-adopters, the means for adopters (4.06) is found to be considerably higher than those of non-adopters (3.53). Almost all of the measured items scored a mean of above 4.00 hence suggesting a high level of agreement by the adopters to the importance of organizational learning culture on information security effectiveness. By having a positive learning

environment, security function of any organization will have the ability to learn on new security mechanisms, identify potential risks brought by new technology, and will have a more positive outlook on the complexity of newly adopted technology such as the BDS (Fichman & Kemerer, 1997).

Measurement Items (Top Management Support)		Adopters (N=15)		Non- Adopters (N=10)	
		Mean	Std. Dev.	Mean	Std. Dev.
TS1	Top management supports the adoption of BDS	3.87	.743	2.80	.400
TS2	Top management accepts possible risks which may result from adopting BDS	3.87	.640	2.80	.622
TS3	Top management takes information security issues into account when planning to adopt BDS	3.87	.743	3.20	1.289
TS4	Top management allocates budget and manpower for information security functions	3.73	.799	2.70	.678
TS5	Top management effectively communicated its support for information security goals associated to BDS adoption	3.87	.640	2.90	.322
	Cronbach's Alpha = 0.919 **Total**	3.84	.267	2.88	.509
	(Information Security Culture)				
SC1	Information security is a key norm shared by the employees of this organization	4.00	.535	3.60	.966
SC2	Employees of this organization value the importance of information security	4.07	.594	4.00	.816
SC3	A culture exists in this organization that promotes good information security practices	3.80	.676	3.40	1.075
SC4	Information security has traditionally been considered an important organizational value	3.87	.834	3.10	1.101
SC5	Practicing good security measures is the accepted way of doing business in this organization	4.20	.561	4.00	.471
SC6	This organization has dedicated efforts to create an information security- focused workforce	4.13	.640	3.10	1.287
	Cronbach's Alpha = 0.839 **Total**	4.01	.440	3.53	.667
	(Organizational Learning Culture)				
LC1	There is an agreement that the organization's security function's ability to learn is the key to information security effectiveness	4.07	.458	3.80	.422
LC2	The basic values of the security function in this organization include learning as key to improvement	4.13	.516	3.80	.789
LC3	The sense around the organization is that employee learning is an investment, not an expense	3.73	.799	3.20	1.229
LC4	Learning is seen as a key commodity necessary to guarantee organizational survival	4.00	.845	3.70	.949
LC5	The collective wisdom in this organization is that once we quit learning, we endanger our future	4.07	.799	3.40	.843
LC6	This organization encourages its employees to pursue security certifications/accreditations	4.33	.488	3.30	.675
	Cronbach's Alpha = 0.740 **Total**	4.06	.490	3.53	.683

Table 3: Descriptive Statistics for Top Management Support, Information Security Culture and Organizational Learning Culture

The means, standard deviations and internal consistencies of the two variables for *Environmental* context are shown in Table 4. As depicted in the table – the mean score for *security and privacy regulatory concerns* shows a small difference between adopters (3.75) and non-adopters (3.87). This study hypothesized that higher concern for security and privacy related regulation

associated to the use of big data will negatively affect the intention to adopt BDS, but the relatively small difference in the mean scores found it to be inconclusive. Thus, based solely on the mean scores, it can be said that both adopters and non-adopters are highly concern on the need to comply with security and privacy regulations. One explanation for this is, organizations that have traditionally worked with high volume of data would have been trained to familiarize themselves with data security and to always be aware of requirements for regulatory compliance. This proposition may especially be true for organizations operating in any highly regulated industries; e.g. finance, healthcare.

Measurement Items (Security and Privacy Regulatory Concerns)		**Adopters (N=15)**		**Non- Adopters (N=10)**	
		Mean	Std. Dev.	Mean	Std. Dev.
RC1	Adherence to security standards and privacy regulations is a challenge with the collection, storage, analysis and reuse of big data	3.93	.704	4.00	1.054
RC2	It is harder to assess the compliance of all personal data collected by BDS with the requirements of data protection law	3.73	.884	3.90	.876
RC3	With the use of BDS, there is a concern of legal implications due to non-compliance to security standards and privacy regulations	3.60	.910	3.70	.823
	Cronbach's Alpha = 0.794 **Total**	3.75	.414	3.87	.521
	(Risks in Outsourcing)				
OR1	The need to outsource BDS creates concerns on data security and privacy	3.47	.915	4.20	.632
OR2	The need to outsource BDS creates vulnerability in access control of the organization's information asset	3.80	.862	3.90	.994
OR3	The need to outsource BDS creates risks through excessive dependency towards vendor	3.20	1.014	3.70	1.160
OR4	The need to outsource BDS complicates the process of implementing corporate policy in protecting individual privacy and data security	3.40	.910	4.00	.667
	Cronbach's Alpha = 0.852 **Total**	3.47	.448	3.95	.498

Table 4: Descriptive Statistics for Regulatory Concerns and Risks in Outsourcing

The means score for *risks in outsourcing* shows a clear difference between adopters and non-adopters (3.47 and 3.95 respectively). While both means are above the uncertain scale (>3.0), the mean is higher and closer to 4.00 (agree scale) for the non-adopters. These results indicate that the non-adopters were more concern about the risks associated with outsourcing practices. The highest mean out of the four measurement items went to OR1, where the non-adopters agreed that the need to outsource BDS creates concerns on data security and privacy. Both adopters and non-adopters seem to have high variances in their answers for OR3, which states that the need to outsource BDS creates risks through excessive dependency towards vendor (std. dev. >1.0). Organizations with prior involvement in outsourcing for example, may have assembled experiences and skills in outsourcing practices. Thus, working with their outsourcing partners were not seen as inviting the risks of excessive dependency – hence possible disagreement of some organizations on item OR3.

5. Conclusion, limitation and future work

This study is a preliminary investigation into BDS adoption from the context of information security. TOE framework is adopted as the conceptual research framework and adapted to

measure information security related factors (Sec-TOE) that may influence organizational intention to adopt BDS. Theoretically, this study contributes to the existing technology adoption framework by conceptualizing security related factors as predictors to BDS adoption by organizations. Besides the usual constructs used in other studies that was based on TOE framework, this study introduces two new constructs under the *Organizational* context; *information security culture* and *organizational learning culture*. Based on descriptive analysis conducted, it is revealed that organizations classified as adopters have a relatively high agreement towards the following adoption determinants; perceived compatibility, top management support, information security culture and organizational learning culture (all four are predicted to have positive effect on intention to adopt BDS). Whilst, the non-adopters were shown to be negatively affected by the following two factors; 1) perceived complexity and 2) risks in outsourcing. Security and privacy regulatory concern was one determinant factor found to be inconclusive. The result shows that both adopters and non-adopters have a very similar level of concern on the need to comply with security and data protection regulations.

While the results of this study demonstrate the path to which the Sec-TOE framework is heading in relation to influencing BDS adoption, more robust data are needed to provide stronger empirical evidence for all the hypotheses. The limitations of this study include a small number of respondents, sampling method used that may not capture the actual view of organizations and incapability to conduct hypothesis testing. As this study is a part of future studies planned, the main objective is to have an initial view on the reliability of the framework. For the next phase, the plan is to conduct a survey with a wider population. The target population are public listed companies in New Zealand and Malaysia. This quantitative study will then be complemented by a single case study aimed to derive further support on how information security may affect the intention to adopt data-intensive technology such as BDS. The case study is also aimed to elicit any other security determinants in BDS adoption that may have been left out in the initial Sec-TOE framework presented in this study.

References

Ahmad Salleh, K., Janczewski, L., & Beltran, F. (2015). SEC-TOE Framework : Exploring Security Determinants in Big Data Solutions Adoption. *PACIS 2015 Proceedings. Paper 203*.

Bansal, A., Kaur, A., & Aggarwal, A. (2014). Big data explosion: Insight for new age managers. *International Journal of Scientific & Engineering Research*, *5*(5), 7–11.

Borgman, H. P., Bahli, B., Heier, H., & Schewski, F. (2013). Cloudrise: Exploring Cloud Computing Adoption and Governance with the TOE Framework. In *2013 46th Hawaii International Conference on System Sciences* (pp. 4425–4435).

Chau, P. Y. K., & Tam, K. Y. (1997). Factors Affecting the Adoption of Open Systems : An Exploratory. *MIS Quarterly*, *21*(1), 1–24.

Cumbley, R., & Church, P. (2013). Is “Big Data” creepy? *Computer Law & Security Review*, *29*(5), 601–609.

Davenport, T. H. (2014). *Big Data at Work: Dispelling the Myths, Uncovering the Opportunities*. Massachusetts: Harvard Business School Publishing Corporation.

Dhillon, G. (1997). *Managing Information System Security*. Hampshire: MacMillan Press Ltd.

Fichman, R. G., & Kemerer, C. F. (1997). The assimilation of software process innovations: an

organizational learning perspective. *Management Science*, *43*(10), 1345–1363.
Gartner Inc. (2014). *Survey Analysis : Big Data Investment Grows but Deployments Remain Scarce in 2014*.
Grover, V. (1993). An Empirically Derived Model for the Adoption of Customer-based Interorganizational Systems. *Decision Sciences*, *24*(3), 603–640.
Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences*, *43*(4), 615–660.
IDG Enterprise. (2014). *Big Data: A Survey* (Vol. 19).
Kshetri, N. (2014). Big data .eraflew remusnoc dna ytiruces ,ycavirp no tcapmi s′ *Telecommunications Policy*, 1–12.
Kwon, O., Lee, N., & Shin, B. (2014). Data quality management, data usage experience and acquisition intention of big data analytics. *International Journal of Information Management*, *34*(3), 387–394.
Lim, J. S., Ahmad, A., & Maynard, S. (2010). Embedding Information Security Culture Emerging Concerns and Challenges. In *PACIS 2010*.
MIT Technology Review. (2015). *Securing the Big Data Life Cycle*. *MIT Technology Review Custom*.
Nambisan, S., & Wang, Y. (1999). Roadblocks to Web Technology. *Communications of the ACM*, *42*(1), 1997–2000.
Nasser, T., & Tariq, R. S. (2015). Big Data Challenges. *Journal of Computer Engineering & Information Technology*, *4*(3), 31–40.
Oliveira, T., & Martins, M. F. (2011). Literature Review of Information Technology Adoption Models at Firm Level. *The Electronic Journal Information Systems Evaluation*, *14*(1), 110–121.
Pahnila, S., Siponen, M., Mahmood, A., Box, P. O., Oulun, F.-, & Siponen, E. M. (2007). Employees ' Behavior towards IS Security Policy Compliance. In *Proceedings of the 40th HICSS* (pp. 1–10).
Rogers, E. M. (2003). *Diffusion of Innovations*. *New York Free Press* (Vol. 21).
Sans Institute. (2015). *Enabling Big Data by Removing Security and Compliance Barriers*.
Schlienger, T. (2003). Analyzing Information Security Culture : Increased Trust by an Appropriate Information Security Culture. In *Proceedings of the 14th International Workshop on Database and Expert Systems Applications*.
Teo, T. S. H., Ranganathan, C., & Dhaliwal, J. (2006). Key Dimensions of Inhibitors for the Deployment Commerce. *IEEE Transactions on Engineering Management*, *53*(3), 395–411.
Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books.
Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476–486.
Wielki, J. (2015). The Opportunities and Challenges Connected with Implementation of the Big Data Concept. In M. Mach-Król, C. M. Olszak, & T. Pełech-Pilichowski (Eds.), *Advances in ICT for Business, Industry and Public Sector* (Vol. 579, pp. 171–189). Cham: Springer Publishing.
Wood, P. (2013, March). How to tackle big data from a security point of view. *Computer Weekly*. Retrieved from http://www.computerweekly.com/